

ADENTRO

Adentro Overview

Adentro provides consumers with an amazing WiFi experience at their favorite spots, while helping to grow local businesses by better engaging and targeting their customers. By offering a branded captive portal for your guest WiFi network, customers are given the ability to opt-in to targeted messaging sent using the Adentro platform.

Adentro Configuration

This document provides basic details necessary for configuring a Cisco Wireless LAN Controller with the Adentro captive portal.

Note: This guide is not compatible with Cisco WAP series APs or EWC.

Identifying Cisco Access Points

Adentro identifies Cisco access points by their wireless MAC address. This can be retrieved via the WLC's UI. Adentro requires the **Base Radio MAC** for each access point that the guest wifi will operate on. The Base Radio MAC can be located in the AP details page under WIRELESS - All APs.

AP Name	IP Address	AP Model	AP MAC	AP ID
CiscoAP00fe.c831.d67c	192.168.0.54	AIR-CAP3702I-A-K9	00:fe:c8:31:d6:7c	4 d,

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Wireless All APs > Details for CiscoAP00fe.c831.d67c

Access Points All APs Radios 802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration Advanced Mesh RF Profiles FlexConnect Groups FlexConnect ACLs 802.11a/n/ac 802.11b/g/n Media Stream Application Visibility And Control Country Timers Netflow

General	Credentials	Interfaces	High Availability	Inventory	Advanced																																														
General <table border="1"> <tr><td>AP Name</td><td>CiscoAP00fe.c831.d67c</td></tr> <tr><td>Location</td><td>default location</td></tr> <tr><td>AP MAC Address</td><td>00:fe:c8:31:d6:7c</td></tr> <tr><td>Base Radio MAC</td><td>00:fe:c8:2e:a3:c0</td></tr> <tr><td>Admin Status</td><td>Enable</td></tr> <tr><td>AP Mode</td><td>local</td></tr> <tr><td>AP Sub Mode</td><td>None</td></tr> <tr><td>Operational Status</td><td>REG</td></tr> <tr><td>Port Number</td><td>1</td></tr> <tr><td>Venue Group</td><td>Unspecified</td></tr> <tr><td>Venue Type</td><td>Unspecified</td></tr> <tr><td>Venue Name</td><td></td></tr> <tr><td>Language</td><td></td></tr> <tr><td>Network</td><td></td></tr> </table>			AP Name	CiscoAP00fe.c831.d67c	Location	default location	AP MAC Address	00:fe:c8:31:d6:7c	Base Radio MAC	00:fe:c8:2e:a3:c0	Admin Status	Enable	AP Mode	local	AP Sub Mode	None	Operational Status	REG	Port Number	1	Venue Group	Unspecified	Venue Type	Unspecified	Venue Name		Language		Network		Versions <table border="1"> <tr><td>Primary Software Version</td><td>7.6.130.0</td></tr> <tr><td>Backup Software Version</td><td>0.0.0.0</td></tr> <tr><td>Predownload Status</td><td>None</td></tr> <tr><td>Predownloaded Version</td><td>None</td></tr> <tr><td>Predownload Next Retry Time</td><td>NA</td></tr> <tr><td>Predownload Retry Count</td><td>NA</td></tr> <tr><td>Boot Version</td><td>15.2.4.0</td></tr> <tr><td>IOS Version</td><td>15.2(4)J86\$</td></tr> <tr><td>Mini IOS Version</td><td>8.0.115.0</td></tr> </table>			Primary Software Version	7.6.130.0	Backup Software Version	0.0.0.0	Predownload Status	None	Predownloaded Version	None	Predownload Next Retry Time	NA	Predownload Retry Count	NA	Boot Version	15.2.4.0	IOS Version	15.2(4)J86\$	Mini IOS Version	8.0.115.0
AP Name	CiscoAP00fe.c831.d67c																																																		
Location	default location																																																		
AP MAC Address	00:fe:c8:31:d6:7c																																																		
Base Radio MAC	00:fe:c8:2e:a3:c0																																																		
Admin Status	Enable																																																		
AP Mode	local																																																		
AP Sub Mode	None																																																		
Operational Status	REG																																																		
Port Number	1																																																		
Venue Group	Unspecified																																																		
Venue Type	Unspecified																																																		
Venue Name																																																			
Language																																																			
Network																																																			
Primary Software Version	7.6.130.0																																																		
Backup Software Version	0.0.0.0																																																		
Predownload Status	None																																																		
Predownloaded Version	None																																																		
Predownload Next Retry Time	NA																																																		
Predownload Retry Count	NA																																																		
Boot Version	15.2.4.0																																																		
IOS Version	15.2(4)J86\$																																																		
Mini IOS Version	8.0.115.0																																																		
			IP Config <table border="1"> <tr><td>IP Address</td><td>192.168.0.54</td></tr> <tr><td>Static IP</td><td><input type="checkbox"/></td></tr> </table>			IP Address	192.168.0.54	Static IP	<input type="checkbox"/>																																										
IP Address	192.168.0.54																																																		
Static IP	<input type="checkbox"/>																																																		
			Time Statistics <table border="1"> <tr><td>Up Time</td><td>4 d 17 h 24 m 04 s</td></tr> </table>			Up Time	4 d 17 h 24 m 04 s																																												
Up Time	4 d 17 h 24 m 04 s																																																		

Create Pre-Authentication ACL

The pre-authentication ACL should allow access to all Adentro portal servers as well as your DNS and DHCP servers.

HTTP and HTTPS access must be permitted to the following IP addresses for gateway.wifast.com:

54.68.53.46

54.68.126.162

54.68.113.153

54.214.242.30

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security Access Control Lists > Edit

AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Access Control Lists Cisco Access Control Lists FlexConnect ACLs

General

Access List Name	Zenreach
Deny Counters	204

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	54.68.126.162 / 255.255.255.255	TCP	Any	Any	Any	Any	262
2	Permit	0.0.0.0 / 0.0.0.0	54.68.113.153 / 255.255.255.255	TCP	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	54.68.53.46 / 255.255.255.255	TCP	Any	Any	Any	Any	253
4	Permit	54.68.126.162 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	248
5	Permit	54.68.113.153 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	0
6	Permit	54.68.53.46 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	235

RADIUS Configuration

The guide linked above configures the controller to use local authentication. You must instead add the Adentro RADIUS servers as AAA auth and accounting servers and configure the WLAN to use them.

RADIUS Authentication

Step 1: In the left pane, expand **AAA**, then **RADIUS**, then click **Authentication**.

Step 2: Set **Auth Called Station ID Type** to **AP MAC Address**.

Step 3: Set **MAC Delimiter** to **Colon**.

Step 4: Click **New**.

Step 5: Enter the information in the tables below.

Step 6: Click **Apply**.

Step 7: Repeat steps 3-5 for the second table.

Server IP Address: 54.69.8.147

Shared Secret Format: ASCII

Shared Secret: 8fc40973252c42e196489d4a16849ff8

Confirm Shared Secret: 8fc40973252c42e196489d4a16849ff8

Port Number: 1812

Server Timeout: 5

Server IP Address: 54.68.29.80

Shared Secret Format: ASCII

Shared Secret: 8fc40973252c42e196489d4a16849ff8

Confirm Shared Secret: 8fc40973252c42e196489d4a16849ff8

Port Number: 1812

Server Timeout: 5

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

security RADIUS Authentication Servers

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
 - DNS
 - Downloaded AVP
- TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
- Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies

Local EAP

Advanced EAP

Priority Order

Certificate

Access Control Lists

Wireless Protection Policies

Web Auth

TrustSec SXP

Local Policies

Advanced

Auth Called Station ID Type: AP MAC Address

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

Framed MTU: 1300

Network User	Management	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	* 54.69.8.147	1812	Disabled	Enabled <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4	* 54.68.29.80	1812	Disabled	Enabled <input checked="" type="checkbox"/>

RADIUS Accounting

Use the same settings as above, but change the port to 1813 for each server.

RADIUS Configuration

Step 1: Open the **WLANs** page.

Step 2: Click **WLANs** in the left pane, and select the WLAN you want to edit.

Step 3: Click the **Security** tab.

Step 4: Click the **AAA Servers** tab.

Step 5: Check the **Enabled checkboxes for Authentication Servers** and **Accounting Servers**.

Step 6: Add the two servers that were just set up under **Authentication Servers** and **Accounting Servers**.

Step 7: Check the **Interim Update** checkbox.

Step 8: Set **Interim Interval to 180**.

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EE

ANs WLANs Advanced

WLANS > Edit 'CiscoProd'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
Server 1	<input checked="" type="checkbox"/> Enabled IP:54.69.8.147, Port:1812	<input checked="" type="checkbox"/> Enabled IP:54.69.8.147, Port:1813	<input type="checkbox"/> Enable
Server 2	<input type="checkbox"/> Enabled IP:54.68.29.80, Port:1812	<input type="checkbox"/> Enabled IP:54.68.29.80, Port:1813	
Server 3	<input type="checkbox"/> Enabled None	<input type="checkbox"/> Enabled None	
Server 4	<input type="checkbox"/> Enabled None	<input type="checkbox"/> Enabled None	
Server 5	<input type="checkbox"/> Enabled None	<input type="checkbox"/> Enabled None	
Server 6	<input type="checkbox"/> Enabled None	<input type="checkbox"/> Enabled None	

RADIUS Server Accounting

Interim Update Interim Interval 180

LDAP Servers

Step 9: Click the Advanced tab.

Step 10: Check the **Enable Session Timeout checkbox** and enter a value of **86400 seconds (24 hours)**.

Step 11: Check the **Client User Idle Timeout checkbox** and enter a value of **3600 seconds (1 hour)**.

Step 12: Set **Client User Idle Threshold** to **0 bytes**.

WLANS > Edit 'CiscoProd'

General Security QoS Policy-Mapping Advanced

Allow AAA Override	<input type="checkbox"/> Enabled	DHCP	<input type="checkbox"/> Override
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled	DHCP Addr. Assignment	<input type="checkbox"/> Required
Enable Session Timeout	<input checked="" type="checkbox"/> 86400 Session Timeout (secs)	EOAP	
Aironet IE	<input type="checkbox"/> Enabled	Split Tunnel (Printers)	<input type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled	Management Frame Protection (MFP)	
Override Interface ACL	IPv4: <input type="text" value="None"/>	MFP Client Protection	<input type="checkbox"/> Optional
Layer2 Acl	IPv6: <input type="text" value="None"/>	DTIM Period (in beacon intervals)	
P2P Blocking Action	<input type="checkbox"/> Enabled	802.11a/n (1 - 255) <input type="text" value="1"/>	
Client Exclusion	<input checked="" type="checkbox"/> Enabled	802.11b/g/n (1 - 255) <input type="text" value="1"/>	
Maximum Allowed Clients	<input type="text" value="0"/>	NAC	
Static IP Tunneling	<input type="checkbox"/> Enabled	NAC State	<input type="text" value="None"/>
Wi-Fi Direct Clients Policy	<input type="checkbox"/> Enabled	Load Balancing and Band Select	
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>	Client Load Balancing	<input type="checkbox"/>
Clear Hotspot Configuration	<input type="checkbox"/> Enabled		
Client user idle timeout(15-1000000)	<input checked="" type="checkbox"/> 3600 Timeout Value (secs)		
Client user idle threshold (0-10000000)	<input type="text" value="0"/> Bytes		

Step 13: Click **Apply**.

External Web Authentication

The WLC may have external web auth enabled globally or on a per-WLAN basis. In both cases the following External Webauth URL must be used:

<https://gateway.wifast.com/cisco/>

Remember to assign the Pre-Authentication ACL created previously to the WLAN.

The screenshot below shows the External Webauth URL set on a per-WLAN basis.

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANs (which is highlighted in orange), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar has a tree structure with WLANS selected, and under WLANS, WLANS and Advanced are listed. The main content area is titled 'WLANS > Edit 'CiscoProd''. It shows the 'General' tab selected, with sub-tabs for Layer 2, Layer 3, and AAA Servers. Under Layer 3, the 'Security' tab is selected. The configuration pane shows the following settings:

- Layer 3 Security: Web Policy
- Authentication (radio button selected):
 - Passthrough
 - Conditional Web Redirect
 - Splash Page Web Redirect
 - On MAC Filter failure
- Preattribution ACL: IPv4 Zenreach, IPv6 None, WebAuth FlexAcl None
- Sleeping Client: Enable (checkbox)
- Over-ride Global Config: Enable (checkbox checked)
- Web Auth type: External(Re-direct to external server)
- URL: <https://gateway.wifast.com/cisco/>

At the bottom, there is a 'Foot Notes' section with two entries:

- 1 Web Policy cannot be used in combination with IPsec
- 2(a) FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

Disable WebAuth SecureWeb and HTTPS Redirection

Make sure the **WebAuth SecureWeb** and **HTTPS Redirection** (only present after firmware version 8.x) settings are disabled, otherwise after clicking the "Connect" button the user will be presented with a SSL error and will be unable to login. This can be resolved by disabling WebAuth SecureWeb and HTTPS Redirection on the controller.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT **COMMAND**

anagement

Summary

SNMP

HTTP-HTTPS

Telnet-SSH

Serial Port

Local Management

Users

User Sessions

Logs

Mgmt Via Wireless

Software Activation

Tech Support

HTTP-HTTPS Configuration

HTTP Access

HTTPS Access

WebAuth SecureWeb

HTTPS Redirection

Web Session Timeout Minutes

Current Certificate

Name:	bsnSslWebadminCert
Type:	3rd Party
Serial Number:	1442843552
Valid:	From Jun 28 00:00:01 2016 GM
Subject Name:	C=US, O=Cisco Systems Inc., C
Issuer Name:	C=US, O=Cisco Systems Inc., C
MD5 Fingerprint:	c9:7f:d3:90:7c:1c:2d:83:33:1a

Make sure the configuration is saved and WLC rebooted after the configuration change.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT **COMMANDS** HELP FEEDBACK

Save Configuration | Ping | Logout

Commands

System Reboot

Save and Reboot **Reboot without Save**

Download File

Upload File

Reboot

Config Boot

Scheduled Reboot

Reset to Factory Default

Set Time

Login Banner

Warning: The configuration of the controller is changed and not saved yet. Click on "Save and Reboot" to save the changes before the controller is rebooted, or click on "Reboot without Save" to reboot the controller without saving the changes. Please be aware that in either case, all the connections will be lost. To regain the connection, please log in again after the controller is rebooted.